

Privacy Vaults Online, Inc. d/b/a/ PRIVO, an authorized Safe Harbor provider under the Children's Online Privacy Protection Act ("COPPA") hereby responds to the Commission's "Questions on the Parental Consent Method" it has published in connection with the application for approval of parental verification method filed by iVeriFly, Inc. on October 25, 2013 (the "Parental Verification Method Application").

**1. Is this method already covered by existing methods enumerated in Section 312.5(b)(1) of the Rule?**

As to the verification aspects of the Application, the methods are already covered. As set out in iVeriFly's Parental Verification Method Application, the iVeriFly service consists of these elements: (1) an email providing "details"<sup>1</sup> of the operator's<sup>2</sup> privacy policy and linking to a form that requests parental name, address and last four digitals of social security number ("SSN"); (2) a verification of parental identity via the last four digits of SSN; (3) a series of "out of wallet" challenge questions; (4) a confirming phone call; (5) a recorded set of keypress responses by which the parent affirms parentage, receipt of disclosures and consent to child registration; and (6) a unique identifier code for the parent to enter on the operator's registration page permitting the completion of registration. In addition, the Parental Verification Method

---

<sup>1</sup> PRIVO notes that the publicly available copy of the Parental Verification Method Application does not provide any information about the "details" that will be given or how they will be presented. Accordingly, PRIVO cannot comment on whether these elements would comply with the operators' notice obligations. The Commission cannot, without that information, determine whether this notice tells the parent what information has already been collected, the uses to which it will be put to, that the parent has the ability to review and request deletion of this data, and other requirements. In this regard, PRIVO notes that there is a difference between third-party parental verification methods and third-party parental consent management methods. The process that the FTC has set up and that iVeriFly is utilizing is designed to approve verification methods. A third-party consent manager has to take some responsibility for the compliance of the users of its service. This demands ongoing auditing and deeper review and approval along the lines of the Safe Harbor process that the FTC has already established. Therefore, this is not the proper vehicle to approve the consent management aspects of the Application, nor is there sufficient information presented to do so.

<sup>2</sup> As used herein, "operator" and "online operator" and "online service" refer to the full range of services and providers covered by COPPA including websites, mobile apps, plug ins, etc.

Application indicates that, once a parent goes through the service's process once, it will not have to do so again at other participating sites. This implies that the service will include a centralized consent management tool as well. While this may be a unique blending together of various facets of available parental verification methods, the underlying methods themselves are already approved and in use by many parties in the industry.

For example, all operators must provide email notice to parents of their privacy policies. Parental verification via SSN is an approved method contained in Section 312.5(b)(1). The Commission has previously approved knowledge based authentication ("KBA") via "out of wallet" challenge questions as a parental verification mechanism. Parental verification via phone calls manned by trained personnel is a method listed in Section 312.5(b)(1). Asking the parent to confirm parentage/guardianship, assigning a unique identifier to a parent who has completed the verification process, and central consent management are nothing new, either. The Commission has seen and approved these elements since at least 2005 when it acknowledged that PRIVO, whose service offers these and other elements, is a Safe Harbor infomediary that acts as a consent manager and offers a variety of proofing methods.<sup>3</sup>

As a result, the only potentially unique element presented in the iVeriFly Application is the use of telephone keypress entries. If iVeriFly were asking for permission to substitute a recorded attendant for a trained operator, then maybe there would be a novel question for the

---

<sup>3</sup> See e.g., 71 FR 13247 (2006) ("Infomediary services act as middlemen in obtaining verifiable parental consent for Web sites and can offer options such as driver's license and social security number verification."). See also PRIVO, Comments, COPPA Rule Review P104503 (June 30, 2010) ("Infomediaries already exist that allow a parent to create a single credential and use that verified credential (from email plus to more reliable verified identity) to permission children's use of online services and participation in marketing initiatives through turn-key registration solutions and through discrete web services.")

Commission to consider, here.<sup>4</sup> But that is not the case. iVeriFly is only using telephone keypress to record parental consent to various disclosures and terms of its service. Given that telephone keypress is a permissible method of signing contracts under the Federal E-Sign Act, appropriately using it to record receipt of disclosures and consent to terms seems a routine matter.

There simply is no reason for the Commission to approve any parental verification method application that is built upon a cobbling together of existing methods. Rather, the Commission should dismiss such requests as moot. The Commission can detail in a dismissal why it considers the request to be moot, but it should not grant a parental verification method application and state that its grant is based on the fact that the constituent elements of the “method” were all previously approved. The Commission’s approval is simply too powerful a statement. As discussed more fully below, the Commission’s grant unduly elevates in importance the “method” set forth in the application and perversely undercuts other implementations of the same methods it has already approved.

A Commission grant of a method portrayed as being “new,” when it is in fact merely an aggregation of existing methods, will be understood in the industry as approving only the particular configuration of these methodologies that the applicant has set forth.<sup>5</sup> Moreover, it will be relied upon by operators as evidence that (1) they must use a method that has received a

---

<sup>4</sup> PRIVO notes that standing alone, the keypress entry method would not be sufficient. In the first place, the phone number could not be collected from the child. But more importantly, the child likely lives in the household with the parent. The child could answer the phone and easily press 1, 2, and 3 in response to prompts.

<sup>5</sup> Website operators and mobile app developers are primarily focused on producing a quality product that provides a positive user experience, and are desperately seeking any authoritative statement that they are “COPPA-compliant.” As a result, they are susceptible to the impression left in the marketplace by the FTC parent verification method approval process. Thus, while PRIVO agrees that KBA should be considered a sufficiently secure method of

grant letter from the FTC, and (2) that by using the approved methodology, the operator will be “COPPA-compliant,” that is, the other obligations of the COPPA Rule, such as data retention, security methodology, and the giving of appropriate notices and the like, will be overlooked.

---

parental verification for use under COPPA, reporting on the FTC’s approval of that method implicitly, and in some cases explicitly, stated that the approval was tied to the applicant’s particular implementation of the method. Consider the following from BloombergBNA which was published a week after the Commission’s decision, when there had been a considerable opportunity to have carefully analyzed the decision before publishing news concerning it:

**FTC Gives Stamp of Approval to COPPA Parental Consent Method by Imperium**

Monday, December 30, 2013

The Federal Trade Commission Dec. 23 announced that it had [approved](#) a verifiable parental consent method under the Children's Online Privacy Protection Rule proposed by Imperium LLC.

The FTC's approval of the consent method proposed by Westport, Conn.-based Imperium follows the commission's rejection in November 2013 of a separate consent method proposed by AssertID Inc. (221 PRA, 11/15/13).

The commission had said AssertID's proposed method did not meet the approval criteria in the COPPA Rule, which implements the Children's Online Privacy Protection Act. AssertID's consent method was based on peer verifications through a parent's social network.

In its latest action, the FTC approved Imperium's proposed use of “knowledge-based authentication” (KBA), which verifies a user's identity “by asking a series of challenge questions,” according to a Dec. 23 statement by the FTC.<sup>5</sup>

<http://www.bna.com/ftc-gives-stamp-n17179881019/>. Almost no amount of further explanation following those opening paragraphs could possibly adequately convey to the reader that the Commission’s approval was not inextricably tied to the implementation of KBA presented by Imperium or undo the impression left by numerous news articles that were published before it.

For example, DataGuidance reported: The FTC approved the application submitted by Imperium, Inc. which provided for a knowledge-based identification (KBA) process as it “offers the individual an opportunity to be verified by answering challenging questions [...] which are difficult for someone other than the individual to answer.” . . . As the method has now been approved other businesses are now also entitled to implement it as an acceptable form of obtaining parental consent. Imperium founder and CEO Marshall Harrison said, “We are gratified to be the only new method approved by the FTC for Verified Parental Consent for COPPA. We look forward to working with the industry to protect children from unsafe practices.” [See http://dataguidance.com/news.asp?id=2183](#). The quoted language is used in a confusing manner and reasonably leads to an impression that the “it” that was approved was only Imperium’s implementation of KBA, rather than KBA more generally.

In another example, PR Newswire carried this: Imperium®, an established industry leader in fraud prevention and identity validation solutions, is pleased to announce that ChildGuardOnline has received approval from the FTC for its knowledge-based authentication method used to obtain verifiable parental consent. This approval signifies that online businesses that request information from children under the age of 13 now have a new, more technologically-advanced option to comply with COPPA. <http://www.prnewswire.com/news-releases/ftc-approves-childguardonlines-new-method-for-parental-consent-verification-239462071.html>.

That is why a deeper review of the applicant's ability to act as a consent manager, assure its users' overall transparency in the consent management process and overall COPPA compliance is necessary and beyond the scope of this approval process.

Avoiding these impressions is particularly important with regard to the iVeriFly Application because iVeriFly lambasts most of the verification methods contained in Section 312.5(b)(1) as being inadequate. For example, iVeriFly states that SSN verification is "unreliable" and further states that verifying identity does nothing to assure that the adult is the child's parent.<sup>6</sup> What iVeriFly is making amounts to a sales pitch as to why potential customers should consider going beyond the minimum of what the FTC's rules require, but that sales pitch tries to call into question the compliance of every operator who has ever used any of the methods enumerated in Section 312.5(b)(1) or any combination of them that is different than the one that iVeriFly proposes. As a result, such operators will feel compelled to similarly seek Commission approval of their particularized implementation of the Section 312.5(b)(1) methods. This impending vicious cycle shows how approving requests that do not introduce truly unique verification methods actually works against the Commission's goals in establishing this process and undermines the flexibility it intended to allow the industry to innovate and take advantage of advances in technology. That is, the more permutations of the same methodologies the Commission considers and approves, the more suspect any implementation that is not specifically blessed by the Commission becomes. Moreover, those methods that are approved will be seen in the industry as providing full COPPA compliance, when there are many other aspects to COPPA compliance that these methods do not even begin to address.

---

<sup>6</sup> Application at 3-4.

**2. If this is a new method, provide comments on whether the proposed parental consent method meets the requirement for parental consent laid out in 16 CFR § 312.5(b)(1). Specifically, the Commission is looking for comments on whether the proposed parental consent method is reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent.**

As noted above, in the main, PRIVO believes that the Parental Verification Method Application does not present a new methodology to be considered under this standard. However, it does propose a follow up telephone call which has the effect of decoupling the verification and consent processes, and potentially limiting its usefulness as a paper trail. That is, a child could answer the follow up telephone call and enter the required keypresses. This could be seen as a step backwards from securing the consent in the same form where the SSN information is collected.

**3. Does this proposed method pose a risk to consumers' personal information? If so, is that risk outweighed by the benefit to consumers and businesses of using this method?**

The proposed service does not allow operators and parents any flexibility in determining how much personal information the parent must give up in connection with the child's participation. The process is arduous and demands a great deal of information. While this may improve reliability of identification of a parent, that level of assurance may be all out of proportion to the need for the consent in the first place. Such a disconnect is anathema to the NSTIC Guiding Principles. Parents may well balk, and begin to withdraw their children from online activity to the detriment of all online operators, if they are asked to give up a large amount of personal information just so their child can receive a personalization newsletter or be allowed to store game scores. This, again, shows why it will set a bad precedent if consent management services are approved based on no more information that is presented in this Application and without any continued FTC oversight of such a service.

Even where more “risky” activities might be involved on a particular operator’s site, it is not immediately clear why so much information beyond SSN is needed. The Parental Verification Method Application notes that almost no child under 12 knows the last four digits of their parent’s SSN. It is even less likely that they know SSN information for any other adult, such as neighbor or friend. Given that fact, why should the parent always also be required to give up answers to multiple challenge questions and their telephone number after having provided the last four digits of their SSN?

In addition, the implication in the Parental Verification Method Application that the service will include a centralized consent management tool, as well as the parent’s ability to block the child’s log in each and every time he or she seeks access to a site where s/he has already registered through the iVeriFly process, indicates that a considerable amount of data retention must be involved. The Application does not recite that parents are given any notice of the iVeriFly privacy policy and practices, that their information will be stored for use in connection with future authentications, and that their child’s attempts to log in to sites that the parent has consented to will be tracked so that the parent can block their sign in at any time.

Finally, iVeriFly offers many other products besides the proposed Parental Consent Verification Method. The Commission must understand how the proposed method will fit into the overall business plan for the company and whether there is any sharing of data across its offerings. By way of example, in the Aristotle safe harbor proceeding, the Commission established privacy safeguards by requiring that Aristotle separate its databases. Similarly, in the safe harbor process, applicants must demonstrate what their business model is to show that they

can stand up a resilient service and to surface any conflicting uses that data collected might be put to. The same sorts of requirements should apply to iVeriFly's Application as well.

## Conclusion

Therefore, PRIVO submits that the instant Parental Verification Method Application is completely inappropriate for the Commission's verification method approval process. It does not present a new method, and the Commission's processes should not be used simply to validate a particular applicant's proprietary business method. Moreover, the Commission should not approve a method if the amount of data it collects is unreasonable or there remain questions as to how that data might be put to use in other aspects of the applicant's business.

Respectfully submitted,

PRIVACY VAULTS ONLINE, INC. d/b/a PRIVO

By:       /s/        
Denise Tayloe, CEO

Dated: January 22, 2014